Symantec Central Quarantine

Symantec Central Quarantine

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Documentation version QS 2.0

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

Trademarks

Symantec and the Symantec logo are trademarks of Symantec Corporation.

Windows is a registered trademark of Microsoft Corporation. Other product names mentioned in this manual may be trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

CONTENTS

About the Symantec Central Quarantine

By default, Symantec and Norton AntiVirus products are configured to isolate infected items that cannot be repaired with their current sets of virus definitions. These items are forwarded to the Central Quarantine.

From the Central Quarantine, the infected samples are submitted to the Symantec AntiVirus Research Center (SARC) for analysis. One of two transport technologies selected at install is used to submit samples:

- Internet-based Scan and Deliver: An automated virus sample submission and definition delivery system that provides realtime protection against heuristically detected new viruses.
- Email-based Scan and Deliver: A virus sample submission and virus definitions delivery system that includes the Scan and Deliver Wizard to simplify sending items to SARC for analysis. If a new virus is found, updated virus definitions are returned by email.

The Symantec AntiVirus Research Center is committed to providing swift, global responses to computer virus threats, proactively researching and developing technologies that eliminate such threats, and educating the public on safe computing practices.

At SARC, a team of virus experts develops identification and detection technology to find and eliminate computer viruses. Aiding the researchers is Symantec AntiVirus Research Automation (SARA). With SARA, a high percentage of virus sample submissions can be analyzed automatically. The virus definitions to remove the virus are created and distributed to customers without human intervention. This technology stops newly discovered viruses before they can spread.

Installation

Three components are installed to create the Symantec Central Quarantine:

- Quarantine Console: Snaps into the Microsoft Management Console (MMC) to perform Central Quarantine management tasks
- Quarantine Server: Stores virus-infected samples and communicates with the Symantec AntiVirus Research Center (SARC)
- Alert Management System (AMS): Manages alerts and notifications triggered by selected Quarantine Server events

The components can be installed on the same or different Windows NT or Windows 2000 computers.

System requirements

You need administrator-level privileges for the computer or domain where you plan to install the Central Quarantine. The following table summarizes the minimum system requirements for the Central Quarantine.

Quarantine Console

- Windows 2000 or Windows NT Server 4.0 with Service Pack 5 or higher
- 128 MB RAM
- Minimum swapfile size of 250 MB
- 12 MB available disk space
- Internet Explorer 5.01 or later
- Microsoft Management Console (MMC) 1.2 or later
  If the proper version of MMC is not already installed, MMC is automatically installed with the Quarantine Console.
- Administrator rights

Quarantine Server

- Windows 2000 or Windows NT Server 4.0 with Service Pack 5 or higher
- 128 MB RAM
- Minimum swapfile size of 250 MB
- 15 MB available disk space

- 500 MB to 4 GB disk space recommended for quarantined items
- Internet Explorer 5.0 or later
- Administrator rights

Alert Management Server

- Windows 2000 or Windows NT Server 4.0 with Service Pack 5 or higher
- 128 MB RAM
- 20 MB available disk space
- Administrator rights

Installing the Symantec Central Quarantine

The installation files for the Symantec Central Quarantine reside in the Digital Immune System (DIS) folder of the distribution CD-ROM.

To install the Quarantine Console:

1. From the \DIS\QConsole folder, run Setup.exe.
2. Follow the on-screen prompts.

   If the proper version of MMC is not already installed, MMC is automatically installed with the Quarantine Console.

To install the Quarantine Server:

1. From the \DIS\QServer folder, run Setup.exe.
2. Follow the on-screen prompts.
3. When prompted, select one of the following:
   - Internet-based Scan and Deliver
   - Email-based Scan and Deliver

   See “Using Internet-based Scan and Deliver” on page 11 and “Using Email-based Scan and Deliver” on page 24 for more information.

   To change from one to the other after install, you must reinstall the Quarantine Server.

To install AMS:

1. From the \DIS\AMS folder, run Setup.exe.
2. Follow the on-screen prompts.

Creating a Central Quarantine

The Central Quarantine has two components:

- Quarantine Server that is installed on any Windows NT/2000 computer to store infected samples and communicate with SARC
- Quarantine Console that snaps into MMC to perform management tasks

To use the Central Quarantine:

- Enable the Quarantine Server.
- Configure forwarding to the Quarantine Server.
- Configure Scan and Deliver to transport samples to SARC and receive virus definitions updates.

Email-based Scan and Deliver or Internet-based Scan and Deliver is selected during the Quarantine Server install. To change from one to the other, reinstall the Quarantine Server.

Enabling the Central Quarantine

Configure the Quarantine Server to act as a centralized repository for infected files that could not be repaired on client computers. Then, configure clients to forward copies of the files contained in their local Quarantines.

For more information on configuring forwarding copies of quarantined files, see “Configuring client forwarding” on page 9.

Note: If you are selecting Symantec Central Quarantine for the first time, follow the procedure in “To select an initial Quarantine server to manage.” If you have already attached to a Quarantine server, follow the instructions in “To change the Quarantine Server to which Central Quarantine attaches.”

To select an initial Quarantine server to manage:

1. In the left pane, click **Symantec Central Quarantine.** If you are opening Symantec Central Quarantine for the first time, you are prompted to attach to This Computer or Another Computer.
2. Do one of the following:
   - To use the local computer as the Quarantine server, click **This Computer**. The word "(Local)" is displayed at the end of Symantec Central Quarantine.
   - To use another computer as the Quarantine server, click **Another Computer**. Type the server name or click **Browse** to locate the computer. Type the username and password for the computer and the domain name, if part of a domain.

To change the Quarantine Server to which Central Quarantine attaches:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Attach to server**.
2. Do one of the following:
   - To attach to the local computer, type the server name and click **OK**.
   - To attach to another Quarantine server, type the server name, enter the username and password to log on to the server, and enter the domain name, if part of a domain.

Configuring client forwarding

Two types of Central Quarantine clients can forward virus samples to the Quarantine Server:

- Managed, such as Norton AntiVirus Corporate Edition clients and servers managed with Symantec System Center
- Nonmanaged, such as Norton AntiVirus for Microsoft Exchange, Norton AntiVirus for Gateways, or Norton AntiVirus for Lotus Notes

A key difference between the two types of clients is how virus definitions updates are returned. Under Email-based Scan and Deliver, virus definitions updates are returned by email for all specified platforms and applied under administrator control.

Under Internet-based Scan and Deliver, virus definitions updates are returned and installed automatically only on computers that are running a managed product. For nonmanaged products, administrators must download and apply updated virus definitions when notified.

For more information about Internet-based Scan and Deliver virus definitions updates, see “Managed and nonmanaged products” on page 16.

To configure managed clients to forward to the Quarantine Server:

1. Right-click clients or servers in the Symantec System Center and click **All Tasks** > **Norton AntiVirus** > **Quarantine Options**.
2. Click **Enable Quarantine or Scan And Deliver**.
3. Click **Allow Forwarding To Quarantine Server**.

   By selecting forwarding, clients cannot submit items directly to SARC from the Quarantine on the client.
4. Under Server Name, enter the server name, IP address, or SPX address of the Quarantine Server.
5. Enter the port and protocol specified when setting the Quarantine Server properties.

   See “Configuring the Quarantine Server” on page 11 for Internet-based Scan and Deliver. See “Configuring the Quarantine Server” on page 24 for Email-based Scan and Deliver.
6. Select an automatic operation to run on the client Quarantine when virus definitions updates arrive.

To configure nonmanaged products to forward to the Quarantine Server:

1. Locate the Quarantine Forwarding settings of the product.

   Refer to the documentation or online help of the product.
2. Enter the server name or IP address where the Quarantine Server is running.
3. Enter the port and protocol specified when setting the Quarantine Server properties.
4. Enter the Retry interval in seconds.

   See “Configuring the Quarantine Server” on page 11 for Internet-based Scan and Deliver. See “Configuring the Quarantine Server” on page 24 for Email-based Scan and Deliver.

Using Internet-based Scan and Deliver

Internet-based Scan and Deliver is an automated virus sample submission and definition delivery system that provides realtime protection against heuristically detected new viruses. All computers worldwide that run Symantec and Norton AntiVirus products are connected to SARC.

Samples of files or boot sectors that might be infected with a new virus are captured on protected computers and sent through the network to the analysis center, which collects and automatically analyzes the samples. If a new virus is found, the center produces and returns new virus definitions, the signatures used to detect, verify, and remove the virus.

New definitions are packaged as updates to Symantec and Norton AntiVirus products and distributed immediately to any customer that reports the new virus. The signatures are later distributed to all other customers to prevent the new virus from spreading further.

Configuring Internet-based Scan and Deliver

Internet-based Scan and Deliver requires two items of information for Central Quarantine operation:

- The folder location to store files on the Quarantine Server
- The appropriate protocols for your network and the port on which to listen

Other settings, including Web communication, sample submission policy, and definition return policy, have default settings carried from install that may be appropriate without modification.

Configuring the Quarantine Server

The Quarantine Server receives virus samples from computers running Symantec and Norton AntiVirus products. The Quarantine Server is the centralized repository for infected files that could not be repaired on client machines. After the Quarantine Server is configured, configure clients to send copies of the files contained in their local Quarantines.

For more information on configuring clients to forward copies of quarantined files, see “Configuring client forwarding” on page 9.

To configure the Quarantine Server:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
2. On the General tab, enter the folder location for the Central Quarantine.
3. Specify the maximum size for the Quarantine.
4. Select the appropriate protocols for your network and specify the port on which to listen.

   Do not use another application’s reserved port. Generally, ports over 1025 are not reserved.

Communicating with the gateway

Web Communication settings determine how the Central Quarantine communicates with the gateway to the SARC analysis center. Generally, the default gateway is supplied when the Quarantine Server is installed.

The sample submission and definitions return transactions can be secured over the Web using Secure Socket Layer (SSL) encryption technology. The encryption level (40-bit or 128-bit) is determined by the version of Internet Explorer installed on the Quarantine Server computer.

To specify Web Communication settings:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
2. On the Web Communication tab, specify settings:
   - Name: Gateway computer that communicates with the analysis center
   - Secure submission: Check to use SSL for submissions
   - Secure download: Check to use SSL for returned virus definitions

Specifying an HTTP firewall proxy

Many sites install the Central Quarantine behind a proxy firewall. Because all transactions with the analysis center gateway are sent by HTTP and secured by SSL, they must be authenticated. To enable communication between the Central Quarantine and the gateway, you must supply a username and password for the firewall proxy, as well as its address and port.

To specify the HTTP firewall proxy:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
2. On the Firewall tab, enter the firewall proxy information:
   - Firewall name: IP address or name of the firewall
   - Firewall port: Port on which to communicate with the firewall
   - Firewall User name: User name
   - Firewall password: Password

Setting a sample submission policy

Sample Policy settings determine whether or not virus samples are submitted automatically to the gateway. If automatic sample submission is not selected, samples in the Quarantine must be released to the gateway individually.

For additional security, specify that user data be stripped from samples before submission.

Policy submission settings can be superseded on an item-by-item basis when viewing the Actions tab for a selected item in the Quarantine.

To set sample policy:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
2. On the Sample Policy tab, set sample policy:
   - Automatic sample submission: If checked, virus samples are automatically queued for analysis
   - Queue check interval: Frequency at which the Quarantine is checked for new items
   - Strip user data from sample: For data security, only the virus portion of the infected file is sent to the gateway
   - Status query interval: Frequency at which the gateway is polled for status changes about submitted samples

Entering Customer Information

Customer Information is included in all messages (virus samples) from customers to gateways. It identifies the customer making the request and is used for authorization and tracking. The information is entered at install, but can be modified if necessary.

To specify Customer Information:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
2. On the Customer Information tab, specify customer information:
   - Company name: Name of company
   - Account number: Symantec support plan account number
   - Contact name: Administrator contact at company
   - Contact telephone: Telephone number with area code
   - Contact email: Required should correspondence be necessary

Managing virus definitions updates

To manage virus definitions updates, set the following policies:

- Definition Policy: How frequently the Central Quarantine polls the SARC gateway for updated, certified virus definitions
- Install Definitions: Which machines receive certified or noncertified virus definitions automatically in response to newly discovered viruses from sample submissions

Virus definitions updates for nonmanaged clients must be downloaded manually.

Setting definition policy

Definition Policy determines how frequently the gateway is polled to download updated certified virus definitions. Certified virus definitions are tested by the analysis center before general release.

Noncertified virus defintions are automatically generated and downloaded by the analysis center in response to a newly discovered virus, according to the installing definitions policy.

To set definition policy:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
2. On the Definition Policy tab, set definition policy:
   - Active sequence number: The sequence number of the currently installed definitions on the Quarantine server. Definitions can be either certified or noncertified.
   - Certified definitions interval: In minutes, how frequently the gateway is polled for updated certified definitions. The default setting (in minutes) is once per day.

Installing definitions

Install Definitions policy determines which computers receive updated virus definitions automatically in response to virus detections.

Separate policies can be set for certified and noncertified virus definitions. Certified virus definitions are tested by the analysis center before distribution. Noncertified virus defintions are automatically generated by the analysis center in response to a newly discovered virus.

If virus definitions are delivered for a virus detected on a computer that is not selected to receive virus definitions automatically, you can manually queue the computer for virus definitions delivery.

To set install definitions policy:

1. In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
2. On the Install Definitions tab, set the install definitions policy:

   Certified definitions

   - Install on selected targets: If checked, certified virus definitions are automatically installed on the selected servers. Click **Select** to specify the servers.

   Definitions that are not yet certified

   - Install on selected clients: If checked, noncertified virus definitions are automatically installed on the computers on which the virus was detected.
   - Install on servers of selected clients: If checked, noncertified virus definitions are installed on the parent server of the infected client.

- Install on selected targets: If checked, noncertified virus definitions are automatically installed on the selected servers. Click **Select** to specify the servers.

Delivery

- Retry interval: In minutes, how frequently virus definitions updates are attempted when targets are disconnected.

To manually queue a computer for definitions delivery:

1 In the right pane, right-click a quarantined item and click **Properties**.

2 On the Actions tab, click **Queue item for definition delivery**. If the item is not eligible for a definitions update, the Queue item for definition delivery button is not available.

Managed and nonmanaged products

Two types of Central Quarantine clients can forward items to the Central Server:

- Managed, such as Norton AntiVirus Corporate Edition clients managed with Symantec System Center
- Nonmanaged, such as Norton AntiVirus for Microsoft Exchange, Norton AntiVirus for Gateways, or Norton AntiVirus for Lotus Notes

The key difference between the two is how virus definitions updates are returned. Virus definitions updates can be installed automatically only on computers that are running a managed product.

Nonmanaged products must be updated manually when virus definitions are created in response to a newly discovered virus. For these products, an alert is generated that contains the location of FTP sites from which to download the virus definitions.

If a nonmanaged product runs under Windows NT/2000, you can install a managed version of Norton AntiVirus Corporate Edition on the same computer. Because both Central Quarantine clients share the same set of virus definitions, the nonmanaged product can forward infected items to the Central Quarantine and the managed product will receive the virus definitions update.

When definitions are available for a nonmanaged product, a “Cannot install definitions on target machines” alert is generated. The alert includes the locations of FTP sites from which virus definitions can be downloaded.

To locate updated virus definitions for nonmanaged products:

1. Right-click the infected item in the quarantine and click **Properties**.
2. On the Errors tab, note the FTP sites from which to download updated definitions.

To configure an alert that includes FTP locations:

1. Right-click **Symantec Central Quarantine** and click **Properties**.
2. On the Alerting tab, configure a Send Internet Mail or Write to Event Log alert for the Cannot install definitions on target machines event.

   An email is sent or an entry is written to the NT event log, respectively.

Reviewing sample submission status

A sample's status within the system can be determined by reviewing the actions performed and attributes set during communications between the Quarantine Server and the gateway.

Viewing a list of quarantined items

Files are added to the Central Quarantine when client machines are configured to forward infected items to the Quarantine Server. The status entry in the table reports the processing state of the sample within the system.

Status	Meaning
Quarantined	Sample has been received by the Central Quarantine.
Submitted	Sample has been submitted to SARC for analysis.
Released	Sample has been queued for analysis.
Held	Sample is withheld from submission.
Unneeded	New virus definitions are not required for the sample.
Needed	New virus definitions are required for the sample.
Available	New virus definitions are held for delivery to the submitting computer.
Distribute	New virus definitions are queued for delivery to the submitting computer.

Status	Meaning
Distributed	New virus definitions have been delivered to the submitting computer.
Installed	New virus definitions have been installed on the submitting computer.
Attention	Sample requires intervention from technical support.
Error	Processing error occurred.
Not installed	Virus definitions could not be delivered to the submitting computer.
Restart	Sample processing will begin again.

To view a list of quarantined items:

- In the left pane, click **Symantec Central Quarantine**.

  Quarantined items are listed in the right pane.

To get detailed information about a quarantined item:

- Right-click an item in the quarantine and click **Properties**.

Interpreting attributes of submissions

Request and response messages exchanged between clients and servers contain numerous attributes that describe a sample and its status within the system. These proprietary attributes always start with the X- characters.

To view attributes for a sample:

1. In the left pane, right-click **Symantec Central Quarantine**.
2. In the right pane, right-click an item and click **Properties**.
3. On the Sample Attributes tab, double-click a displayed attribute for a brief definition.

Reviewing actions on samples

The actions taken on a sample include a selected sample's submission and virus definition delivery status.

You can override the default sample submission policy settings for the selected sample. You can manually queue a sample for submission to the analysis center, as well as query for updated virus definitions files for the selected sample.

To view sample actions:

1 In the left pane, click **Symantec Central Quarantine**.

2 In the right pane, right-click a quarantined item and click **Properties**.

3 On the Actions tab, review actions taken on the sample.

Reviewing submission errors

Submission errors, if any, are reported for each sample. Review the entries to determine the action required for the sample.

To review submission errors:

1 In the left pane, right-click **Symantec Central Quarantine**.

2 In the right pane, right-click an item and click **Properties**.

3 On the Errors tab, review submission errors.

Overriding automatic operation

Policy settings for automatic sample submission and virus definitions install can be overridden.

Generally, samples are submitted manually only after a submission error or a change to the queue priority of selected samples is desired. Similarly, if virus definitions are available for a computer that is not selected to receive virus definitions automatically, you can manually queue the computer for virus definitions delivery.

Submitting files manually

Suspect files can be manually submitted for virus analysis. To be eligible for manual submission:

- The sample cannot already be eligible for automatic submission. The X-Sample-Priority must be 0.

  To manually set the priority for a sample, right-click an item in the Quarantine, click Properties, and set the Submission priority on the Actions tab.

- The sample has not already been submitted (X-Date-Submitted is missing or 0).

- The sample has not already been analyzed (X-Date-Analysis-Finished is not present or 0).

To manually submit items to the analysis center:

1. In the Quarantine, select one or more files.
2. Right-click the selection and choose **All Tasks > Queue item for automatic analysis**.

Requesting virus definitions updates manually

A target machine that does not receive virus definitions updates automatically can be queued for delivery of new virus definitions. For these machines, the sample status is Available. To be eligible for manual definitions delivery:

- The sample cannot already be eligible for automatic delivery of virus definitions (X-Signatures-Priority is 0).
- The sample requires virus definitions (X-Signatures-Sequence > 0).
- The sample has not yet been disinfected (X-Date-Sample-Finished is missing or 0).

To request virus definitions updates:

1. In the Quarantine, select one or more files.
2. Right-click and choose **All Tasks > Queue for automatic delivery of new definitions**.

Sending alerts

In addition to entries in the Quarantine Log, alerts triggered by Central Quarantine events can be sent in the following ways:

- Message box
- Page
- Email
- Broadcast
- Written to NT event log

For nonmanaged clients that do not receive virus definition updates automatically, the “Cannot install definitions on target machines” alert is generated. The alert is posted automatically to the Error tab of the infected item with the locations of FTP sites to download the definitions and the

Quarantine Log. If enabled, the Send Internet Mail and Write to Event Log alerts also include this information.

Configuring alerting

Alerting settings determine the events at the Quarantine that trigger alerts and where to send them. Each event can be enabled or disabled individually.

Event	Meaning
Unable to connect to the Gateway	Cannot connect to the Immune System gateway.
Defcast error	Defcast is the service that distributes new virus definitions from the Quarantine Server to target machines.
Cannot install definitions on target machines	Distribution of new virus definitions failed. Also indicates that virus definitions are available for nonmanaged clients.
Unable to access definition directory	Quarantine Server cannot find the virus definitions directory.
Cannot connect to Quarantine Scanner svc	Samples cannot be scanned in the Quarantine and will not be forwarded to the gateway.
The Quarantine Agent service has stopped	Quarantine will not be able to communicate with the gateway.
Waiting for needed definitions	Virus definitions have not yet arrived from the gateway.
New Certified definitions arrived	New certified virus definitions have arrived on the Quarantine Server.
New non-certified definitions arrived	New noncertified virus definitions have arrived on the Quarantine Server in response to a sample submission.
Disk quota remaining is low for Quarantine dir	The Quarantine folder is becoming full.
Disk free space is less than Quarantine max size	The Quarantine folder is set to a maximum size greater than the available free disk space.

Event	Meaning
Sample: was not repaired	Either a sample wasn't repaired or a repair wasn't necessary.
Sample: unable to install definitions	New virus definitions could not be installed, usually due to a corrupted virus definitions set.
Sample: processing error	There was an error processing this sample.
Sample: needs attention from Tech Support	Sample could not be processed automatically. Contact Tech Support for help with the sample.
Sample: held for manual submission	Sample is being held on the Quarantine Server instead of being automatically submitted.
Sample: too long without installing new defs	New virus definitions should have been installed (status is available), but were not.
Sample: too long with Distributed Status	New virus definitions have arrived from the gateway, but confirmation that they were installed on the client has not yet been received at the Quarantine.
Sample: too long with Needed status	Virus definitions have not yet been pulled from the gateway.
Sample: too long with Released status	Gateway has not yet responded.
Sample: too long with Submitted status	Sample has not yet been accepted by the gateway.
Sample: too long with Quarantined status	Sample has not yet been scanned initially at the Quarantine.
Sample: new definitions held for delivery	New virus definitions are being held on the Quarantine Server instead of being delivered.

After identifying the AMS server, specify who receives the alert for each event. After the recipients are configured, each event can be enabled or disabled separately on the Alerting tab.

To configure alerting:

1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.

2 On the Alerting tab, configure alerts.

To specify who receives an alert and by what method:

1 On the Alerting tab, click **Configure**.

2 Select an event and click **Configure**.

3 Click **Help** on each panel of the wizard for more information.

Using Email-based Scan and Deliver

Email-based Scan and Deliver is a virus sample submission and virus definitions delivery system that protects against heuristically detected new viruses. It includes the Scan and Deliver Wizard to simplify sending items to SARC for analysis.

If a new virus is found, updated virus definitions are returned by email, where they can be applied first in the Central Quarantine to test and confirm operation. The updated virus definitions are then applied to clients and servers throughout the network.

Configuring Email-based Scan and Deliver

Email-based Scan and Deliver requires two items of information for Central Quarantine operation:

- The folder location to store files on the Quarantine Server
- The appropriate protocols for your network and the port on which to listen

Configuring the Quarantine Server

Configure the Quarantine Server as a centralized repository for infected files that could not be repaired on client computers. Once this is done, you can configure clients to send copies of the files contained in their local Quarantines.

For more information on configuring clients to forward copies of quarantined files, see "Configuring client forwarding" on page 9.

To configure the Quarantine Server:

1 Right-click **Symantec Central Quarantine** and click **Properties**.

2 On the General tab, enter the Quarantine folder location.

3 Specify the maximum size for the Quarantine.

4 Select the appropriate protocols for your network and specify the port on which to listen.

Do not use another application's reserved port. Generally, ports over 1025 are not reserved.

Submitting files for analysis

Quarantine includes the Scan and Deliver Wizard to simplify sending items to SARC for analysis. Optionally, your personal data is stripped from the file copies that are sent to SARC to ensure privacy.

Once you receive the virus definitions update by email you can apply it first in the Central Quarantine to test and confirm its effectiveness. Next, apply the update to the client computer (where the original infected file remains quarantined). The client computer then performs a selected preset operation such as repairing the infected item and releasing it from the client Quarantine automatically.

Sending files to SARC

The Scan And Deliver Wizard simplifies sending items to SARC for analysis. Scan and Deliver emails the virus strain to Symantec for analysis and immediate virus definition creation.

When you click Submit Item, the Scan And Deliver Wizard analyzes the file and may recommend an action other than delivering it to SARC. For example, the virus might be eliminated with your current set of virus definitions. You can override the recommended action and submit it.

Note: You must have an Internet connection and an email address to submit files to SARC.

To submit a file to SARC:

1. Open the Symantec Central Quarantine.
2. Right-click a file in the list of Quarantined items and click **Submit Item to SARC**.
3. Follow the directions in the Scan And Deliver Wizard to collect information and submit the file to SARC for analysis.
4. When the wizard runs, there are two settings to cover special circumstances:
   - Strip File Content: If selected, only the portion of a file that can be infected is sent to SARC. Any confidential data is stripped from the document before it is submitted. The complete file, however, remains in Quarantine.

- Specify Custom SMTP Server: This setting applies to corporate environments to route items from Quarantine to SARC through your custom SMTP server.

Managing quarantined files

By default, Symantec and Norton AntiVirus clients are configured to isolate infected items that cannot be repaired with their current sets of virus definitions. Clients that have been configured to forward these infected files automatically send copies to the Central Quarantine Server.

Once the files are in the Central Quarantine, the following administrative actions are possible:

- View a list of quarantined files
- Repair files
- Restore files
- Delete files
- Submit files to SARC for analysis

Viewing a list of quarantined items

Files are added to the Central Quarantine when client computers are configured to forward infected items to the Central Quarantine. You can view a list of the files contained in the Quarantine Server.

To view a list of quarantined items:

- In the left pane, click **Symantec Central Quarantine**.

To get detailed information about a quarantined item:

- In the right pane, right-click an item and click **Properties**.

Deleting quarantined files

Although you can delete any item in the Central Quarantine, reserve this option for files you no longer need. After confirming that updated virus definitions detect and eliminate the virus, it is safe to delete the quarantined item.

To delete files:

1 In the left pane, click **Symantec Central Quarantine**.

2 In the right pane, select one or more files in the list of quarantined items.

3 Right-click the selection and click **Delete**.

Repairing and restoring quarantined files

When you click Restore, no attempt is made to repair the file. Use this option with discretion to avoid infecting your system. For example, only use Restore when SARC notifies you that a submitted file is not infected. Restoring a potentially infected file is not safe. Restored files are copied to the Quarantine Console computer.

When you click Repair, an attempt is made to repair the file. You are prompted for a location to store a successful repair. With new virus definitions, you can test the repair in the Central Quarantine before distributing the definitions.

To repair an infected file:

1 In the left pane, click **Symantec Central Quarantine**.

2 In the right pane, select one or more files in the list of quarantined items.

3 Right-click the selection and click **Repair.**

Updating Central Quarantine virus definitions

Because the Quarantine itself performs virus scanning and repairs, you must have current virus definitions. For Email-based Scan and Deliver, the virus definitions reside on the computer where the Quarantine Console is installed.

If SARC returns updated virus definitions by email in response to a submitted virus sample, apply them to the computer where the Quarantine Console is installed. For Email-based Scan and Deliver, you can test the updated virus definitions in the Central Quarantine before applying them to other supported Symantec and Norton AntiVirus products.

If a client version of Norton AntiVirus is installed on the same computer as the Quarantine Console computer, the client version of LiveUpdate will update the Quarantine as well. If not, you must manually apply updated virus definitions.

Symantec supplies updated virus definitions on the the SARC Web site.

To download updated virus definitions:

1. Go to the SARC Web site:

   http://www.sarc.com
2. Click **Definition Updates**.
3. Click **Download Virus Definition Updates**.
4. Select the virus definitions update for Norton AntiVirus Corporate Edition.

To manually install the latest virus definitions:

1. Do one of the following:
   - Detach the virus definitions package emailed from SARC and copy it to any folder on the Quarantine Console computer.
   - Download the virus definitions update and copy it to any folder on the Quarantine Console computer.
2. From a My Computer or Windows Explorer window, locate and double-click the virus definitions update.
3. Follow all prompts displayed by the update program.

   The update is installed in the proper folder automatically.

Testing the virus definitions update

To test updated virus definitions files:

- In the list of Quarantined items, select one or more files.
- Right-click the selection and click **All Tasks > Repair Item**.

After you've confirmed that the new virus definitions eliminate the viruses from files in the Quarantine, apply the definitions to other supported Symantec and Norton AntiVirus products. The same package can be used for Windows NT clients. Additional packages are sent in appropriate formats for other platforms that were specified at the time of submission to SARC. For example, script packages are returned for the Solaris platform.